The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/31/2020

SUBJECT:
A Vulnerability in F5 BIG-IP Edge Client for Windows Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in F5 BIG-IP Edge Client for Windows, which could allow for remote code execution. F5's BIG-IP is a family of products covering software and hardware designed around application availability, access control, and security solutions. Successful exploitation of this vulnerability allows for remote unauthenticated attackers to execute arbitrary code in the context of the application used to browse a specially-crafted web-page. This vulnerability may result in complete system compromise.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- F5 BIG-IP APM 15.x versions prior to 15.1.0.4
- F5 BIG-IP APM 14.x versions prior to 14.1.2.6
- F5 BIG-IP APM 13.x versions prior to 13.1.3.4
- F5 BIG-IP APM 12.x versions prior to 12.1.5.1
- F5 BIG-IP APM 11.x versions prior to 11.6.5.3
- F5 BIG-IP APM 7.x versions prior to 7.1.9
- F5 BIG-IP Edge Client for Windows

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in F5 BIG-IP Edge Client for Windows, which could allow for remote code execution. F5 BIG-IP Edge Client for Windows is prone to a memory-corruption vulnerability that occurs due to a use-after-free error. Specifically, this issue exists in the 'ActiveX' component of the affected application. An attacker can exploit this issue by enticing an unsuspecting user into visiting a specially-crafted web-page using the 'Microsoft Internet Explorer' web-browser. Attackers can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely cause denial-of-service conditions. Successful exploitation of this vulnerability allows for remote unauthenticated attackers to execute arbitrary code in the context of the application used to browse a specially-crafted web-page. This vulnerability may result in complete system compromise.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by F5 to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
F5:
https://support.f5.com/csp/article/K20346072
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5897